United States Department of Education

Federal Student Aid

Student Aid Internet Gateway (SAIG)
System Security Plan

Version 1.0
November 8, 2002

RECORD OF CHANGES

Page No(s)	Change Comments	Date of Change	Author
Entire Plan	Version 1.0 – First Draft	November 8, 2002	Mod Partner

TABLE OF CONTENTS

1.0 System Identification

The first section of the plan provides basic identifying information about SAIG. It contains general descriptive information regarding who is responsible for SAIG, its purpose, and its sensitivity level.

1.1 System Name/Title

Name: Student Aid Internet Gateway
Unique identifier: SAIG
System Category: General Support System

1.2 Responsible Organization

1.2.1 Federal Organization

Federal Student Aid (FSA)
U.S. Department of Education
830 First Street, NE, Third Floor
Washington, DC 20202

1.2.2 System Maintainer

Accenture
One Freedom Square
11951 Freedom Drive
Reston, VA 20191

NCS Pearson - Modernization Partner
2510 North Dodge Street
Iowa City, Iowa 52240

Computer Sciences Corporation – VDC owner/operator
2100 East Grand Ave.
El Segundo, CA 90245

1.3 Information Contacts

The table below lists the SAIG contacts for FSA, NCS Pearson and CSC.

Name	Organization	Role	Phone	Email Address
Andrew Boots	FSA	Computer Security Officer (CSO)	202.377.3559	andrew.boots@ed.gov
Lydia Morales	FSA	FSA Sponsor	202.377.3589	lydia.morales@ed.gov
Tawanda Hampton	FSA	FSA Security Officer (SSO)	202.377.3575	tawanda.hampton@ed.gov
Colleen Ward	Accenture	Project Manager	703.947.2980	colleen.m.ward@accenture.com
Justin Thoensen	NCS Pearson	NCS Manager	319-665-7809	thoeju@ncs.com
Jerry Ryznar	Computer Sciences Corporation	VDC Operations Account Manager	202.842.7397	gryznar@csc.com
Gary Adams	Computer Sciences Corporation	VDC Operations Service Delivery Manager	202.842.8614	Gadams2@csc.com
Jim Cunningham	FSA	VDC SSO	202.377.3577	James.Cunningham@ed.gov

1.4 Assignment Of Security Responsibility

Name	Organization	Role	Phone	Email Address
Tawanda Hampton	FSA	FSA Systems Security Officer	202.377.3575	tawanda.hampton@ed.gov

See SSO Security Notebook for SSO assignment letter.

1.5 System Operation Status

1.5.1 Operational

All three of the components (TD Engine, TDAccess, TDCommunityManager) of SAIG are operational. SAIG went into the operational phase in September 2001.

1.5.2 Under Development

None

1.5.3 Undergoing Major Modification

No component of SAIG is currently undergoing a major modification. The last major modification was when SAIG was upgraded in 2001 from Title IV Wide Area Network (TIVWAN).

1.6 General Description/Purpose

SAIG promotes the electronic exchange of Title IV information over the Internet by providing telecommunications support and "electronic mailboxes" for the delivery and receipt of this information between Title IV applications and user organizations. It is a modified Commercial-Off-The-Shelf (COTS) application from bTrade, Inc. and is made up of the following core components:

- TDNgine – An open architecture gateway that is used as the 'mailbox' application for sending, storing and retrieving data.

- TDAccess – The client software used to send and receive batch FTP data transmissions securely over the Internet using SSL 3.0 and the Diffie-Hellman Dynamic Key Exchange algorithm. TDAccess offers Title IV destination points and Application Systems a simple integration into existing systems. Client software includes Edconnect (for PC users) and TDClient (for Mainframe and Midrange users), which calls the TDAccess API that resides on the HP-UNIX server to send/receive data. Non-PC destination points including Title IV Application Systems integrate the TDAccess client into batch programs/processes. TDAccess supports the following platforms and versions:

  - Win95/98/2000/NT*
  - MVS 2.6.0*
  - SUN Solaris 2.6/2.7
  - IBM AIX 4.2+
  - HP-UX 10+*
  - OS400
  - SCO Unix 4.3+
  - Open VMS 7.1+
  - DEC Unix (True64) 7.2+

  *Note: 99% of SAIG's existing user base uses Windows (including 95, 98, NT, and 2000), MVS, or HP-UX operating systems.

- TDCommunityManager – Product used to manage Title IV destination point mailboxes and data. It runs as a thin client and is accessed via the Web. Users of the system include system administrators, customer service staff, and Title IV destination points. Destination points can use this system to manage their mailboxes and to view network traffic via the Web.

The internal and external users of SAIG include postsecondary institutions, third party servicers, state agencies, guaranty agencies, lenders, banks, ED, and Title IV application system contractors.

The data transmitted over SAIG comes from a variety of different Title IV Application Systems (considered to be Major Applications by FSA). Those Title IV Application Systems are also considered services users can choose to participate in when they enroll with SAIG. They currently include:

- Common Origination and Disbursement (COD): COD is the schools main interface into the FSA system. It receives school disbursement information for student level federal financial aid and validates aid payments to schools.

- Central Processing System (CPS): CPS confirms students' eligibility for Federal student financial assistance; calculates the estimated family contribution (EFC); calculates eligibility for Federal aid (i.e., determine financial need); reports eligibility information to applicants, schools, and guarantors; and supports management information and analysis requirements of other FSA managers and staff.

  There are four applications used to submit Free Application for Federal Student Aid (FAFSA) data to CPS; namely, FAFSA on the WEB (FOTW), FAFSA Express, EDExpress, and paper based forms.

  Using data contained on the FAFSA forms, CPS calculates the EFC for each applicant and the applicant's eligibility for Federal grants, work-study, subsidized loans, or unsubsidized loans. Prior to determining the EFC and calculating eligibility, CPS performs matches of applicant data with other Federal databases to ensure that the applicant is not barred from eligibility. These matches are with:

  - National Student Loan Data System: Identifies applicants in default on previous Federal student loans or who owe overpayments on any Federal Title IV aid program.
  - Selective Service System: Identifies applicants eligible for, but not registered for, the draft.
  - Immigration and Naturalization Service: Validates the applicant's immigration status.
  - Social Security Administration: Confirms applicant's name and social security number.

- Department of Justice: Identifies applicants who are not eligible for student aid because of convictions for drug trafficking or possession.

CPS works hand in hand with EDExpress, a microcomputer-based software package distributed by FSA to schools to support aid packaging, Federal Pell Grant and Federal Direct Loan origination, SSCR, and draw down of data from CPS for use in other school applications. Enrollment services include Renewal Applications, Initial Applications, ISIRs, and Corrections.

- Direct Loan Origination System (DLOS): The Direct Loan Origination System (LOS). COD replaced DLOS functionality beginning with the 02-03 award year; therefore, only Direct Loan information prior to 02-03 travels over SAIG to DLOS.

- Direct Loan Servicing System (DLSS): DLSS manages the direct loan repayment process. The system setup loan services account, upon receipt of the student's promissory note and the school's disbursement notice, and tracks repayments. Direct Loan Delinquency Reporting service allows Direct Loan institutions to supervise their loan default management activities with an electronic version of the ED-supplied Borrower Delinquency Report. This report is available in two formats via SAIG: 1) Report Format and 2) Data Format. Schools may exercise the option to receive the report in either or both formats or not to receive the report at all.

- e Campus Based (eCB): eCB manages Title IV campus based aid requested by schools. It processes FISAP (Fiscal Operations Report and Application to Participate) data received and calculates funding for each school for the Federal Perkins Loan , Federal Supplemental Educational Opportunity Grant (FSEOG), and Federal Work-Study program. This information must be submitted using SAIG.

- Financial Management System (FMS): FMS is a single FSA-wide, integrated financial management and reporting system. FMS provides FSA with single-point contact for program funding and financial data. The system tracks Title IV invoicing, funding, servicing, and collecting processes.

- National Student Loan Database System (NSLDS): NSLDS is a national database of student-level and loan/grant-level data on Title IV programs. The system tracks data on the Federal Family Education Loan Program (FFELP), Federal Direct Loan Program (FDLP), Campus-Based Program loans and grants, Federal Pell Grants, and Federally Insured Student Loans. The NSLDS is intended to provide a research database and to support operational functions that include pre-screening Title IV aid applicants for eligibility, tracking and reporting Student Status Confirmation Reports (SSCR), providing Financial Aid Transcript (FAT) information to schools, calculating cohort default rates for FFELP and FDLP schools, supporting reasonability tests on lender and guarantor billings to FSA, performing borrower tracking, and support for reporting under the Credit Reform Act..

All institutions that participate in the Title IV federal student financial aid programs must have at least one destination point for NSLDS services, which include online financial aid transcript information, Student Status Confirmation Reports functions for updating student enrollment data, overpayment reporting, and borrower tracking. NSLDS has two distinct service categories: 1) Batch services and 2) On-line services that encompass the individual services mentioned above.

- PELL/Regional Financial Management System (PELL/RFMS): COD replaced PELL/RFMS functionality beginning with the 02-03 award year. Only PELL information prior to 02-03 travels over SAIG to RFMS.

- Participation Management (PM): Sub-system of CPS. PM creates and maintains user participation in SAIG for all the different enrollment service options available. The PM also controls the initiation and maintenance of mailboxes on the SAIG Portal. Web enrollment, a subset of the PM subsystem, enables SAIG users to control their participation through an Internet Web site. Existing destination points can add a new user under their current profile, while existing users have the ability to update enrollment services via the Internet. The mainframe-based Participation Management subsystem coexists with the Web site, since interactions between the Internet site and SAIG enrollment databases is vital.

  Potential SAIG users enroll through the Participation Management subsystem. Enrollment may be accomplished by either the hardcopy SAIG Enrollment Form or via the fsawebenroll.ed.gov Web site. Once either the hardcopy document or signature pages from the Web site are processed and released (within 48 hours of receipt), a user id and customer number (when applicable) are assigned and mailed to the user.

  Users electronically download the appropriate software and documentation via the fsadownload.ed.gov Web site. The contents of software and documentation are dependent upon which enrollment services they have requested.

  Once users have received their information and are ready to start processing Title IV data for the Application Systems in which they have enrolled, they are required to contact CPS/WAN Technical Support and perform a short test transmission. Once this test is completed successfully, users then employ the EDconnect software (or appropriately provided mainframe/mid-range TDAccess software) to transmit (send and/or receive) data from their various enrolled services/Application Systems.

Below is a table of the type of information that is processed (sent back-and-forth) between SAIG and each of the interconnected systems.

System	Type Of Information Processed Between Systems
COD	Financial and Privacy Act protected information.
CPS	Financial and Privacy Act protected information.

CPS/PM	Privacy Act protected information.
DLOS	Financial and Privacy Act protected information.
DLSS	Financial and Privacy Act protected information.
eCB	Financial information.
FMS	Financial and Privacy Act protected information.
NSLDS	Financial and Privacy Act protected information.
PELL/RFMS	Financial and Privacy Act protected information.

Below is a table of the type of information that is processed (sent back-and-forth) between SAIG and both the internal and external user organizations.

User Organization	Type Of Information Processed with SAIG
Postsecondary Institutions	Financial and Privacy Act protected information.
Third Party Servicers	Financial and Privacy Act protected information.
State Agencies	Privacy Act protected information.
Guaranty Agencies	Financial and Privacy Act protected information.
Lenders	Financial and Privacy Act protected information.
Banks	Financial and Privacy Act protected information.
NCS Pearson	Sends Privacy Act protected information as part of its roll in the enrollment process for SAIG through PM. They don't send or receive any information over SAIG, in their role as Administrators/Developers, but they do have the ability based on their user rights to view Financial and Privacy Act protected information
Accenture	Does not send or receive any information over SAIG, but does have the ability based on user rights to view Privacy Act protected information through TDCommunityManager.
FSA	Does not send or receive any information over SAIG, but does have the ability based on user rights to view Privacy Act protected information through TDCommunityManager.
NCS Pearson	Does not send or receive any information over SAIG, but does have the ability based on user rights to view Financial and Privacy Act protected information.

1.7 System Environment

SAIG Portal and the TDCommunityManager reside on systems that are physically housed and maintained at the Virtual Data Center (VDC) in Meriden, Connecticut. The

systems used for SAIG development/failover for these two components also reside at the VDC. Computer Sciences Corporation (CSC), under contract with FSA, owns and operates the facility and is responsible for the operation, maintenance, and security of this system from a hardware and Operating System perspective, with the support of Accenture and NCS Pearson staff for application administration and maintenance. The remaining supplementary PM system is maintained at the NCS Pearson facility located in Iowa City, Iowa.

SAIG Portal and TDCommunityManager reside on an HP-UNIX (HPL16) midrange and an NT 4.0/IIS (SFANT014) servers, respectively. There are no dial-up lines directly to either of the servers. The following table lists the physical location, software, hardware, use/functionality and the communication resources for each of the two aforementioned systems. See Appendix A for a logical network diagram.

Server Name	HPL16	SFANT014
Physical Location	VDC	VDC
Software on Server	• Oracle Database v8.1.7 • MQ Series Server v5.2 • bTrade EAclient API • HP-UX v11.0 • Computer Associates TNG • Cisco Local Director • HP Service Guard	• SecureManager 2000 • Oracle Application Server • Online SecureManager Software • JDK (Java Development Kit) • Java Mail • JAF (Java Activation Framework) • JRUN (Enterprise Edition) • CA-TNG Monitoring Agent • Tripwire Client • ArcServe Client • Norton Antivirus
Hardware/OS	HP-UX Midtier	Compaq DL380/NT 4.0
Use/Functionality	Destination Point (Mailboxes)	SaigPortal IIS Webserver
Type Of Communication Resources	Internet and Intranet	Internet and Intranet

See Appendix B for a list of additional software on the HP-UX midtier.

SAIG's development environment coexists with the production hardware. The development servers enjoy the same security as the production servers within the VDC.

Because SAIG primarily resides at the VDC, its communication lines will benefit from the same controls that already exist for the security of the VDC network and other systems and applications operating there. These controls include:

- BMC Enterprise Security Station© (NT servers)
- Tripwire for Servers© (NT servers) – System scanner, Host intrusion detection
- Symantec Norton Anti-Virus© (NT servers)
- Pretty Good Privacy© (UNIX servers) – Encryption software
- BMC Enterprise Security Station© (UNIX servers)
- Computer Associates TNG (UNIX & NT servers) – Access Control
- CheckPoint Firewall-1© (network)
- ISS RealSecure© Intrusion Engine (network)
- TACACS© router authentication software

SAIG software and all of its components were implemented under a normal time schedule.

SAIG, because of the role it plays between Title IV destination points, resides on an open network and can be accessed from overseas. However the general public does not have access due to the registration process that must be followed to obtain a username and password.

1.8 System Interconnection/Information Sharing

The chart below contains information about all SAIG's interconnected systems.

System	Direction	Data Transfer Method	Type Of Interconnection	System Owner/Channel	System Of Record (Y/N)
COD	Bi-directional	MQ	TCP/IP	Schools	Y
CPS	Bi-directional	Batch	TCP/IP	Students	Y
CPS/PM	One way	Batch	TCP/IP	Students	Y*
DLOS	Bi-directional	Batch	TCP/IP	Schools	Y
DLSS	Bi-directional	Batch	TCP/IP	Students	Y
eCB	Bi-directional	Batch	TCP/IP	Schools	N
FMS	Bi-directional	MQ	TCP/IP	FSA CFO	Y
NSLDS	Bi-directional	Batch	TCP/IP	Schools	Y

System	Direction	Data Transfer Method	Type Of Interconnection	System Owner/Channel	System Of Record (Y/N)
PEPS	Bi-directional	Batch	TCP/IP	Schools	N
PELL/RFMS	Bi-directional	Batch	TCP/IP	Schools	Y

*PM is a sub-system of CPS and contains Privacy Act protected information.

FSA is in the process of beginning its Certification and Accreditation (C&A) program for their systems so there was no written management authorization obtained prior to connecting and/or sharing sensitive data or information between SAIG and the system interfaces identified above. FSA is scheduled to begin C&A in 2003, with SAIG certification in quarter one (Q1) of 2004.

Each of the Major Applications that are interconnected with SAIG have SSPs. Please see their respective SSPs for their:

- Written Rules of Behavior (RoB) – Section 2.3 Rules of Behavior
- Security controls – Section 1.7 System Environment

SAIG plays much the same role as a traditional mailbox. As such, when looking at the confidentiality, integrity, and availability of the interconnected systems there are no major security concerns that should be considered for each of the interfaces in the protection of SAIG.

For confidentiality, SAIG does not read each message because each message is compressed and encrypted so the confidentiality level is LOW. The integrity of the information is also LOW because again, SAIG only passes and stores the information. Even though the information passing through the system may be Privacy Act protected, SAIG does not view the data. Availability of the interconnected systems is also LOW. SAIG's mailboxes will function with or without the systems that are interconnected, although interconnected systems may be impacted by an interruption in SAIG's functionality.

The following table lists the sensitivity level, criticality and the date this information was last updated for each of SAIG's interconnected systems. For the information each of these systems possess, see Section 1.6 *General Description/Purpose* of this SSP.

GSS/MA Name	Type (GSS or MA)	Mission Criticality	Information Sensitivity			Last Inventory Update
			Confidentiality	Integrity	Availability	
SAIG	GSS	Important*	High	High	Medium	July 29, 2002
COD	MA	Critical	High	High	Medium	July 29, 2002

GSS/MA Name			Information Sensitivity			
CPS	MA	Critical	High	High	Medium	July 29, 2002
DLOS	MA	Critical	High	High	Medium	July 29, 2002
DLSS	MA	Critical	High	Medium	Medium	July 29, 2002
eCB	MA	Important*	Low	Medium	Medium	July 29, 2002
FMS	MA	Important*	High	High	High	July 29, 2002
NSLDS	MA	Critical	High	High	High	July 29, 2002
PELL/RFMS	MA	Important*	High	Medium	Medium	July 29, 2002
PEPS	MA	Critical	Low	Medium	Medium	July 29, 2002

* Criticality reclassified based on Critical Infrastructure Survey completed in August 2000.

1.9 Applicable Laws or Regulations Affecting the System

The following laws, regulations or policies establish the requirements for confidentiality, integrity and availability for SAIG:

- Computer Fraud and Abuse Act of 1986 (Public Law 99-474).
- Computer Security Act of 1987, Public Law 100-235, 101 Stat. 1724.
- Federal Manager's Financial Integrity Act of 1983 (Public Law – 97-255).
- Freedom of Information Act of 1974, 5 United States Code 552, Public Law 93-502.
- Privacy Act of 1974 (Public Law 93-579).
- OMB Circulars A-123, A-127, A-130.
- Office of Postsecondary Education (OPE) Computer Security Policies and Procedures.
- Information Technology Management Reform Act (ITMRA) of 1996.
- Guidance for Preparation and Submission of Security Plans for Federal Computer Systems that Contain Sensitive Information, OMB Bulletin 90-08 .
- Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18.
- Guidelines for Automatic Data Processing, Physical Security and Risk Management (FIPS PUB 31).
- Guidelines for Documentation of Computer Programs and Automated Data Systems (FIPS PUB 38).
- Computer Security Guidelines for Implementing the Privacy Act of 1974 (FIPS PUB 41).
- Guidelines for Security of Computer Applications (FIPS PUB 73).
- Guidelines for ADP contingency Planning (FIPS 87).
- Guidelines for Computer Security Certification and Accreditation (FIPS PUB 102).
- Standards for Password Usage (FIPS PUB 112).
- U.S. Department of Education *Information Technology Security Manual*, November 1994.

1.10 General Description of Information Sensitivity

All applications/systems require protection for confidentiality, integrity, and availability. The level of protection required is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of SAIG to the organization's mission, and the economic value of SAIG's components. The sensitivity and criticality of the information stored, processed by, or transmitted by SAIG provides a basis for its value and is one of the major factors in risk management. A description of the types of information handled by SAIG and an analysis of the criticality of the information is required. This description and analysis will assist in designing security controls, facilitating security audits, and implementing security countermeasures. Criticality and Sensitivity are defined below.

Criticality Objective	Description
Confidentiality	The information requires protection from unauthorized disclosure.
Integrity	The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to, Authenticity (Verification that the content of a message has not changed in transit) and Non-repudiation (Verification of the origin or receipt of a message).
Availability	The system or data must be available and accessible on a timely basis to meet mission requirements or to avoid substantial losses.

Sensitivity Level	Description
High	A critical concern for the automated information resource. Extremely grave injury occurs to organization interests if information is compromised; could cause loss of life, imprisonment, major financial loss, or require legal action for correction.
Medium	An important concern, but not necessarily paramount in the organization's priorities. Serious injury accrues to organization interests if the information or asset is compromised; could cause significant financial loss or require legal action for correction.

Sensitivity Level	Description
Low	Some minimal level of security is required, but not to the same degree as the previous two categories. Injury occurs to organization interests if the information or asset is compromised; would cause only minor financial loss or require only administrative action for correction

SAIG's Critical Infrastructure Protection (CIP) Survey completed in August 2000 states that SAIG's criticality is **Mission Important**. SAIG was once considered mission critical, according to the *Department of Education Inventory Submission Form* completed in January 2001 and a Risk Assessment conducted in June 2002 but, because of the CIP survey was reclassified.

The inventory submission form for SAIG and its Risk Assessment dated June 2002 stated that the data criticality objective and sensitivity levels are as follows: **Confidentiality** is **High**, **Integrity** is **High**, and **Availability** is **Medium**. The descriptions below were provided by SAIG's *Inventory Submission Form* and documented in the Risk Assessment dated June 2002.

Confidentiality ¾ High. The data transmitted and received by SAIG includes the following Privacy Act data to be maintained with the highest degree of confidentiality: User names, addresses, Social Security Numbers (SSNs), and user personal information (e.g., date of birth and mother's maiden name).

Integrity ¾ High. SAIG data consists of the information provided by the user, including Social Security Number and mother's maiden name. Unauthorized modification of the Privacy Act data could result in incorrect decisions. Therefore, the SAIG data must be maintained with a *high degree* of integrity.

Availability ¾ Medium. SAIG is online 24 hours a day. Short delays (e.g., 2 to 3 days) should not cause critical difficulties and would not severely impede ED's mission in supporting the Title IV aid programs. As such, the availability of the SAIG data is moderately critical to ED's mission and should be maintained with a *medium degree* of availability.

The overall sensitivity level is determined by the highest value for confidentiality, integrity, and availability. Therefore, the overall sensitivity level for SAIG is **High**.

As the above explanation identifies, SAIG will maintain privacy act data and mission critical FSA data. Due to the nature of the data, the following ratings were assigned for the application's sensitivity/criticality.

Confidentiality	Integrity	Availability
High	High	Medium

2.0 Management Controls

Management Controls focus on the management of the IT security system and the management of risk to the system. These controls encompass techniques and concerns that are normally addressed by FSA and SAIG management.

2.1 Risk Assessment and Management

A Risk Assessment was conducted for SAIG in June 2002. It took into consideration the value of the system, threats, vulnerabilities, and the effectiveness of current and proposed safeguards.

The value (criticality and sensitivity) for SAIG was determined by using the CIP survey completed in August 2002 (for criticality) and the Inventory Submission form completed in July 2002. See section 1.10 *General Description of Information Sensitivity* in this SSP.

The threats and vulnerabilities for SAIG can be found in the Risk Assessment for SAIG. Due to the sensitive nature of a Risk Assessment, detailed information will not be provided here, however an overview follows.

No (0) high-risk findings were identified for SAIG. High risk is defined as an exploitation of an identified vulnerability by a threat that will severely and adversely affect SAIG's tangible and intangible resources. This level of risk indicates a critical need for corrective measures and actions. A plan must be developed to incorporate these actions immediately (preferably 0 - 3 months maximum).

Three (3) medium risk findings were identified for SAIG. Medium risk is an exploitation of the identified vulnerability by a threat that will moderately affect SAIG, indicating the loss of some tangible assets or resources, which could impede SAIG's mission, reputation, or interest. This level of risk indicates that corrective actions are needed and that a plan must be developed to incorporate these actions within a reasonable period of time (recommended 3 – 6 months maximum).

Three (3) low risk findings were identified for SAIG. Low risk is when an identified weakness may be subject to exploitation by a threat, but the probability of exploitation is low, and the impact on SAIG would be minor. This level of risk indicates that SAIG management should be cautioned and corrective measures applied where required.

The findings from the risk assessment are being addressed by FSA.

2.2 Review of Security Controls

KPMG Consulting, Inc. prepared an evaluation of the FSA (then SFA) Systems Security and Privacy Risk Management and Control Environment with recommendations for improvement in the form of a September 2000 *Corrective Action Plan (*for the TIVWAN system*)*.

Booz-Allen Hamilton performed the Risk Assessment for SAIG in June 2002.

A Self-Assessment as part of the Government Information Security Reform Act (GISRA) was conducted in June 2002.

SAIG has never undergone an OMB A-130 independent audit review in its current form. Its predecessor, TIVWAN, underwent an A-130 review conducted by KPMG LLP in 2000.

The VDC underwent vulnerability scans in June of 2002. The VDC does not allow SAIG or any other system to conduct either penetration tests or vulnerability scans.

2.3 Rules of Behavior

Rules of Behavior for NCS Pearson staff can be found in section 2.3 of the CPS SSP dated July 2002.

There are no Rules of Behavior specific to SAIG.

2.4 Planning for Security in the Life Cycle

All the components of SAIG are in the Operational/Maintenance phase.

2.4.1 Initiation Phase

A sensitivity assessment was conducted in January 2001 for SAIG. It was validated in June 2002 by conducting a Risk Assessment. See section 1.10 of this SSP for more information on the sensitivity of SAIG.

2.4.2 Development/Acquisition Phase

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

> *15) When SAIG (or any of its components) was in the development/acquisition phase of the life cycle, were:*

- *Appropriate security controls and associated test and evaluation procedures documented and were these tests performed prior to procurement.*
- *The requirements that permits updating the security requirements as new threats/vulnerabilities identified and as new technologies are implemented.*

2.4.3 Implementation Phase

16) When SAIG (or any of its components) was in the implementation phase of the life cycle, was a design review and systems test had been performed prior to placing the system into operation and whether the tests were fully documented, updated, and maintained in FSA's records. Include:

- *Information about additional design reviews and systems tests for any new controls added after the initial acceptance tests were completed and*
- *Whether the documentation of these reviews and tests have been kept up-to-date and maintained in FSA's records.*

2.4.4 Operation/Maintenance Phase

SAIG (and its components) are in the operation/maintenance phase of the lifecycle.

The security operations and administration, operational assurance and auditing and monitoring for SAIG are all services provided by the VDC.

The security operations and administration of the NT systems includes the VDC standard build documentation. This includes security patch installation, security policy implementation (changing of user rights), and setting of logon policy (i.e. Password expiration, length, and uniqueness). The VDC provides operational assurance by conducting daily server checks each morning to ensure server operation. These checks include viewing event logs, NIC card status, loading websites or application, and checking Insight Manager. Conducting audits and monitoring of the NT systems includes checking the audit logs and using TNG monitoring to ensure optimum uptime.

The HP-Unix server is managed per the International Standards Organization (ISO) security procedures for its operation and administration procedures. Operational assurance is maintained by following the ISO operations document that describes proper change control procedures (see VDC SSO for ISO document GPES/UNIX/NE/002). Auditing and monitoring of SAIG's HP-Unix server is performed through the use of TNG software.

2.4.5 Disposal Phase

Section 2.4 (Planning for Security in the Life Cycle) of the VDC Security Plan dated June 1, 2002 states; "Ordinarily, magnetic materials are degaussed and physically destroyed before their disposal." SAIG and its components will follow similar procedures when the time comes.

2.5 Authorize Processing

FSA is in the planning stages of its C&A program. FSA has yet to authorize any system for processing, but expects to initiate and complete C&A packages for all of its systems in 2003 with the help of Xacta's Web-based C&A tool.

Xacta's Web-based C&A tool is a COTS application that automates the security certification and accreditation process. The software simplifies certification and accreditation and reduces costs. The user defines the network or system configuration and the environment in which it operates, and the application automatically engages the appropriate security requirements according to government and/or industry best practices. The software then automatically generates the appropriate test procedures, processes the test results, produces a risk assessment, and allows the user to automatically publish a complete C&A package, including all appendices. Additionally, the software creates a repeatable process.

3.0 Operational Controls

Operational controls address security methods that focus on mechanisms that are implemented and executed primarily by people (as opposed to systems). These controls are put in place to improve the security of SAIG. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

3.1 Personnel Security

3.1.1 Contractor and Subcontractor Personnel Security

All contractor and subcontractor personnel, who participate in the design, operation, or maintenance of SAIG systems or facilities, are subject to FSA's security clearance policy. The security requirements are defined in *U.S. Department of Education Personnel – Suitability Handbook*, Chapter 2, Number 11. The VDC Security Department is responsible for recommending clearance levels appropriate for each position at the VDC. Supervisory personnel at NCS Pearson who have sufficient knowledge of duty assignments, recommend position sensitivity requirements for their employees. SAIG's SSO approves the sensitivity levels assigned to each position.

The following lists the three FSA security clearance levels, which positions will be classified under:

- **High Risk (Level 6C).** These are positions that have the potential for exceptionally serious impact because they involve duties that are critical to FSA. Employees may not assume duties in high-risk positions until their security clearance has been completed and approved by FSA. Employees who are awaiting clearance approval may assume duties at a less sensitive level. Positions requiring high-risk security clearance include Account/Service Delivery Managers and the Resource Access Control Facility (RACF) administrators.
- **Moderate Risk (Level 5C).** These are positions that have the potential for moderate to serious impact. This includes staff responsible for the direction, planning, design, operation, and maintenance of computer systems. Employees in these positions have their work reviewed by someone at level 6C to ensure the integrity of the system. Employees may assume duties in these positions as soon as the clearance paperwork has been submitted. Positions requiring moderate-risk security clearance include database administrators and group managers.
- **Low Risk (Level 1C).** These are positions that require access to computer systems. Employees may assume duties in these positions as soon as their clearance paperwork has been submitted. Programmers and computer operators require low-risk clearance.

As described above employees in either the 1C (low risk) or 5C (moderate risk) levels may begin work after security clearance paperwork is submitted. If the final

investigation does not result in approval, the user must be removed from their positions and their system accesses revoked.

There is no provision for interim access for 6C (High Risk) positions EXCEPT under special arrangement with the Department of Education's OCIO Security, ED's OIG Security Office, the ED Project Manager, the System's Security Officer, and the FSA Personnel Security Officer. If interim 6C access is granted, it is based on such factors as the level of supervision of the interim user and the level of clearance of those supervisory officials overseeing the interim user.

A VDC security administrator will ensure that all CSC employees who need regular access to the VDC fill out the necessary forms. The NCS Pearson Administrative Services Department does the same for their staff. The completed forms are sent to the SSO for approval. Upon receiving SSO approval the VDC or NCS Pearson will then create the appropriate user access.

The necessary forms, based on security level, include:

High Risk (Level 6C):

- SF 85P Questionnaire for Public Trust Positions
- SF 85P-S Supplemental Questionnaire For Selected Positions
- FD 258: Fingerprint Card on file
- Form 306: Declaration for Federal Employment
- Notice of Criminal Liability Under the Privacy Act.
- Signed Rules of Behavior
- Fair Credit Reporting Act Release

Moderate Risk (Level 5C):

- FD 258: Fingerprint Card on file
- Form 306: Declaration for Federal Employment
- Notice of Criminal Liability Under the Privacy Act.
- Signed Rules of Behavior
- Fair Credit Reporting Act Release

Low Risk (Level 1C):

- FD 258: Fingerprint Card on file
- Form 306: Declaration for Federal Employment
- Notice of Criminal Liability Under the Privacy Act.
- Signed Rules of Behavior

<u>Terminating VDC User Access</u>

When employees are removed (terminated) from a VDC position for any reason, VDC management takes the following actions:

- Revokes all access authorizations and immediately notifies the COTR and application CSO of the removal and the termination date.
- Revokes card key access and retrieves badges allowing access to system facilities.
- Reviews with departing employees their obligation to protect system and FSA data and information as required by the Privacy Act.
- All employees must be escorted at all times upon termination.
- Changes all passwords and authorization codes providing access to general staff of controlled system facilities.

Terminating NCS Pearson User Access

When employees from NCS Pearson no longer require access to the system, an email from the Human Resources Department notifies Technical Support and Administrative Services to revoke the user's account. In the event of a full-time employee's voluntary termination or relocation the email identifying the departing employee and the last date of work is sent to Technical Support and Administrative Services. If the employee termination is involuntary, these departments are called immediately and the email will follow.

The employee's termination checklist includes returning company property and deactivation of user IDs and facility access cards. Security administration personnel are responsible for suspending and/or removing the accounts.

If an NCS Pearson or subcontractor employee is removed from a key SAIG position:

- The Administrative Services Team is notified.
- All SAIG-specific keys and badges are retrieved.
- All SAIG access authorizations are removed.
- FSA is notified of the termination.

If necessary, combinations are changed on locks to which the terminated employee had access.

Separation Of Duties

The VDC provides a realistic guarantee that sufficient segregation of duties is maintained. All customers of the Data Center specify segregation of duties between FSA customers and data center personnel in their contracts.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

> *22) Are users access restricted (least privilege) to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform the job?*

23) Are critical functions divided among different individuals (separation of duties)?

SAIG accounts for contractors/subcontractors are provided to individuals, not to institutions. Every user gaining access to SAIG is required to have an individual account with a unique user ID. The mechanism for holding these users accountable for their actions is with the use of audit trails. The audit trails record each attempted user-resource interaction with the user ID and password, which allows each individual's actions to be audited. See section 4.4 Audit Trails in this SSP for further details.

3.1.2 User Organizations Personnel Security

All SAIG user organizations, referred to as destination point administrators (DPAs), must complete an enrollment document (hardcopy or electronically via fsawebenroll.ed.gov) to participate in SAIG services. By completing an application, user organizations will be enrolling individuals as DPAs for destination points (mailboxes) on SAIG. Enrollment is designed to secure the integrity of data that is exchanged between users and the many services accessed via SAIG. Before beginning to complete the application, users determine the SAIG services that their organization must access, the appropriate people who need to interact with those services, and the number of destination points required. Each mailbox must be assigned an individual to serve as its DPA.

Each DPA is required to sign a signature page, which contains the required agreements and notices of Privacy Act statements. Each DPA must read and sign this statement. The original signature page must be attached to the completed hard-copy enrollment form, or with the web signature page containing a confirmation number if submitted via the enrollment Web site, and submitted to SAIG.

Every user requesting access for a DPA must also have a signature from their authorizing official at their organization. For each DPA, the chief officer of the organization (President, CEO, Chancellor, or Designatee) must sign this certification statement. If the organization is a third party servicer acting on a school's behalf, both the school's chief officer and the organization's chief officer must sign. The original signature page must be attached to the completed form, or with the web signature page containing a confirmation number if submitted via the enrollment Web site, and submitted to SAIG.
Original signature documents and other correspondence are sent to:

CPS/WAN Technical Support
P.O. Box 30
Iowa City, IA 52244

Or to their overnight address:

CPS/WAN Technical Support
2510 North Dodge Street

Iowa City, IA 52245

Except in the case of some NSLDS services, the DPA can give access to the enrolled services of a mailbox to multiple individuals called SAIG users. Where permitted, the DPA will determine the SAIG users that are allowed access to that mailbox. The DPA must enforce the security requirements as outlined in the SAIG User Statement (https://www.sfawebenroll.ed.gov/PMEnroll/index.htm), including the completion and maintenance of this statement(s). The President/CEO/Chancellor/Designatee must certify that each DPA has developed secure procedures in compliance with the security requirements for permitting other people to use his/her mailbox. The DPA also must complete a profile for each SAIG user within the EDconnect software used to connect to SAIG.

The process for requesting, establishing, issuing, and closing user accounts is controlled by PM and is not covered in this SSP. See the CPS security plan for this information.

3.2 Physical and Environmental Protection

The Meriden facility uses the Proximity key card system to restrict access to the building and all applicable rooms. The Proximity key card is a radio frequency key that releases a lock mechanism at doors. The Physical Security controls the distribution of all key cards. The Key Card Administrator updates the access list on the Proximity Key Card computer. See section 3.2 Physical and Environmental Protection and Appendix B in the VDC SSP dated June 2002 for more detailed procedures and explanations.

General building security at the NCS Pearson Iowa City facility is provided by an on-site contract security agency, 24 x 7, 365 days a year. Public access is restricted to guarded entrances. A visitor entering the building must sign in and be escorted at all times.

Access to NCS Pearson facilities is restricted. Permanent employees are issued coded, digitized access cards that must be used for entrance to the buildings. Each permanent employee's card has an identification photograph laminated to it. A color-coded grid on the card identifies the restricted access areas each employee is allowed to enter. Temporary employees have similar cards, the difference being that their building access is limited to the calendar year displayed on the right side of the card.

If access cards are forgotten, NCS Pearson Iowa City uses the Access Control/Security System software to bring up individuals' badge records. This allows personnel issuing interim badges to compare the badge photo on file with the individual requesting the badge and also to determine is that individual is still a valid employee. If the system were down, then an identifying photo ID of the individual requesting the interim badge would be required.

If the individual does not have a photo ID, or if his or her name is not on the appropriate roster, the department manager must be contacted to personally identify the individual

before entry will be granted. If the employee doesn't know the name of his or her department or manager (or if the manager/supervisor is not available), Human Resources or Administrative Services must be contacted for assistance.

When an employee, outsource person, or visitor is in an NCS Pearson facility, that person's access card or identification badge **must** be visible (above the waist) on his or her person **at all times**. The visitor badges are returned on a daily basis. Escorts are provided for visitors and guests in NCS Pearson facilities.

The NCS Pearson Computer Operations Department also employs card reader access and is available only to employees authorized by the Data Center Manager. In place are:

- Card keys for building and work-area entrances
- Twenty-four hour security officer coverage
- Cipher locks
- Raised floor in computer room
- Dedicated cooling system
- Humidifier in tape library
- Emergency lighting in computer room
- Fire extinguishers rated for electrical fires
- B/C rated fire extinguisher
- Smoke, water, and heat detectors
- Emergency power-off switch by exit door
- Surge suppressor
- Emergency replacement server
- Zoned dry pipe sprinkler system
- Uninterrupted power supply for LAN servers
- Power strip/suppressors for peripherals
- Power strip/suppressors for computers
- Controlled access to file server room

In summary, SAIG relies on the VDC and NCS Pearson's Iowa City facility for its Physical and Environmental protection. Therefore SAIG is covered under CSC and NCS Pearson facility policies and procedures for the following:

- The physical access control measures in place including those to restrict the entry and exit of personnel from system facility areas (see above).
- The fire safety devices in the buildings that house the system.
- The failure of supporting utilities including electric power, heating and air-conditioning systems, water, sewage, and other utilities.
- The procedures and plans to be followed in the event of a structural collapse.
- The procedures and plans to be followed in the event of a plumbing leak.
- The procedures and plans to be followed if data is intercepted.

SAIG does not use mobile or portable systems.

3.3 Production, Input/Output Controls

The VDC is not responsible for operating the system applications and consequently has no control over marking, handling, labeling, processing, distribution, storage, and disposal of input and output information and media specific to the system.

However the VDC is responsible for the Disaster Recovery Tape Management.
The VDC manages the operation of the offsite tape vaults for disaster backup tapes. The VDC uses the Vault Management System (VMS), which is a subset of the Tape Library Management System (TLMS) from Computer Associates. Two different operators verify all tapes that are sent to and returned from the offsite facility. Mainframe and midrange systems (NT and UNIX platforms) tape librarians are tasked to load tapes, file tapes, track off-site tapes, and audit and inventory vaults for correctness. Offsite personnel only accept tapes from authorized persons displaying the correct access identification. Manual audits of both onsite and offsite vaults are performed periodically. VDC personnel attempt to resolve any variance between the manual audit and tape logs immediately. Tape disposal procedures require all tapes to be degaussed and destroyed before disposal to prevent accidental exposure of the information contained therein.

NCS Pearson has a User Services Support Manager, Technical Support, reporting directly to the SAIG Program Manager. The functions of the User Services Support Manager are as follows:

- Provide for user service support to FSA, SAIG destination points, and the user organizations that support FSA and the SAIG destination points.
- Manage user relations.
- Determine user support requirements.
- Produce and maintain management information regarding user requests.

A staff of technical support representatives is assigned to respond to phone calls from the SAIG user community. The staff supports all aspects of the SAIG program, including user-based software, distribution of SAIG software and materials and enrollment and participation. Technical support can be reached by calling CPS/WAN Technical Support 1-800-330-5947 or by emailing them at: cpswan@ncs.com

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

28) Please answer the following as they relate to NCS Pearson and SAIG.

- *Procedures to ensure unauthorized users cannot read, copy, alter, or steal printed or electronic information.*

- *Procedures to ensure only authorized personnel pick-up, receive, and deliver input and output information and media.*
- *Describe audit trails for the receipt of sensitive inputs/outputs.*
- *Procedures for restricting access to input and output products.*
- *Procedures and controls used for transporting or mailing media or printed output.*
- *Describe the internal and external labeling procedures (including those with special handling instructions).*
- *Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.*
- *Procedures for shredding or other destructive measures for hardcopy media when no longer required.*

- The NCS Inventory control team is responsible for the receipt, storage, and issuance of all inventory items associated with SAIG. This team provides weekly reports of material usage and receipt of incoming items. The team also provides physical counts of material and salvages outdated or erroneous material and is responsible for the transportation of large shipments of materials when necessary as required. Should operations require it, the team members assist in determination of the most economical or effective method of shipment.

- NCS Pearson employs the services of Kenwood Records Storage for secure off-site storage of CPS materials. The company is located at:

  Kenwood Records Storage
  4001 44th Avenue, SW
  Cedar Rapids, Iowa 52404

  Kenwood Records Storage is a commercial records storage company that specializes in the storage of computer records with 24-hour accessibility, 7 days a week. The company employs the following security features:
  - Storage is provided in climate-controlled vaults specifically designed for all media (computer tapes, disks, microfiche, microfilm, etc.).
  - The site has the following security measures in place: a Halon 1301 fire suppression system, a smoke/heat fire alarm system, motion detectors, and door alarm contacts.
  - Monitoring of all building security systems, including fire alarms, motion detectors, and door alarm contacts, is performed by Mid America Alarm Service of Cedar Rapids, Iowa. Mid America Personnel remotely monitor these system 24 hours a day, 7 days a week.
  - Bonded personnel perform all pickup and delivery services.
  - Off-site backup files are rotated on a weekly basis. This rotation is automatically controlled by the vault management feature (VMS) of the tape management system. VMS uses a slotting technique to keep track of tapes stored in locations other than the main NCS Pearson tape library.

VMS is run each week to provide a list of tapes to be moved to the off-site location and a list of tapes to be returned from the off-site location. NCS Pearson uses this facility to control the rotation of off-site SAIG system backup tapes.

- NCS Pearson employs three techniques to sanitize electronic media:
  - overwriting, degaussing and destruction.
  - The Data Center runs daily computer jobs that scratch expired tape and disk data sets.
  - Media Creation Department staff magnetically erases data from magnetic media.

3.4 Contingency Planning (Continuity of Support & Disaster Recovery)

SAIG documentation for this section was being developed during the creation of this SSP. All Contingency Planning, Disaster Recovery, and Continuity of Support documentation for SAIG will be completed on December 10, 2002. Upon completion this plan will be updated with summary information.

3.5 Hardware and System Software Maintenance Controls

FSA IT Security and Privacy Policy states that SAIG's SSO has the responsibility to make sure that contingency plans and other associated documentation are updated to reflect any system changes, which are required annually. The policy also restricts against illegal use of copyrighted software or shareware and contains provisions for individual and management responsibilities and accountability, including penalties.

All test data for SAIG is made-up data. No real or "live" data is used in testing SAIG.

Users computers are outside of the scope of FSA and SAIG and are governed by EDnet. Therefore, refer to the EDnet policy for information about products and procedures, including periodic audits of users' computers (PCs) to protect against illegal use of software and ensure only legally licensed copies of software are installed.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

29) Describe the hardware and system software maintenance controls (in place or planned).

30) What procedures are in place to ensure that maintenance and repair activities are accomplished without adversely affecting system security?

31) Discuss the restrictions/controls on those who perform maintenance and repair activities.

32) Discuss special procedures for the performance of emergency repairs and maintenance.

33) Discuss the procedures used for items serviced through on-site and off-site maintenance.

34) What are the procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.

35) Discuss version control that allows association of system components to the appropriate system version.

36) What are the procedures for testing and/or approving system components prior to promoting to production?

37) Has an impact analyses been conducted to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software?

38) Discuss change identification, approval, and documentation procedures.

39) How are emergency fixes handled?

40) Describe the policies for handling copyrighted software or shareware.

3.6 Integrity Controls

Network

The VDC network uses a CheckPoint Firewall-1©. The CheckPoint firewall is a state-full inspection router and software. An ISS Real Secure© intrusion detection engine monitors and scans the network for changes in files and access rights. Changes of the system configuration are measured by hash counts. All events are written to an audit log that resides on a secure hard drive. The network component of the VDC participates in frequent penetration testing.

NT

All VDC NT systems use Norton Anti-Virus software for virus detection and elimination. Norton Anti-virus runs automatically each Friday at 5:15PM and virus definition updates also occur automatically at 8PM on Fridays. Tripwire for Servers© intrusion detectors are also used to monitor the NT systems for change and hacker intrusion. The Tripwire software uses a collection of one-way hash functions to detect file and system changes. The Tripwire for Servers© database, policy file, and report files can be cryptographically sealed via 1024 bit El-Gamal encryption algorithm. The CSC Computer Emergency Response Co-ordination Center (CERCC) is monitored for the latest information on NT bugs and fixes. The NT System Administrators patch the servers on a proactive basis. Patches are also applied when CERTS indicate that there is an NT security vulnerability.

UNIX

The native UNIX operating system provides adequate protection against all viruses. Tripwire for Servers© is used as the intrusion detector for UNIX systems. The Tripwire software uses a collection of one-way hash functions to detect file and system changes. The Tripwire for Servers© database, policy file, and report files can be cryptographically sealed via 1024 bit El-Gamal encryption algorithm. The UNIX System Administrators patch the servers on a proactive basis. Patches are also applied when CERTS indicate that there is a significant UNIX security vulnerability.

By using CA's TNG software for system performance monitoring on both the NT and Unix systems, each systems performance is analyzed in real time in order to look for availability problems, including active attacks, and system and network slowdowns and crashes.

According to FSA's *IT Security and Privacy Policy* the use of password checkers or crackers must be authorized by SAIG's system administrator. At this time SAIG does not use password checkers/crackers on any of its components.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

Enrollment

42) What controls provide assurance to users that their information has not been altered and that the system functions as expected?

43) Do you scan for viruses? If so, are there procedures for updating virus signature files and automatic and/or manual virus scans?

44) Are reconciliation routines used by the system, such as checksums and hash totals?

46) Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? (Techniques include consistency and

reasonableness checks and validation during data entry and processing. A description of the integrity controls should be included.)

47) Is message authentication used to ensure that the sender of a message is known and that the message has not been altered during a transmission? Include whether message authentication has been determined to be appropriate for your system.

3.7 Documentation

VDC

The VDC is an ISO 9000 certified facility and as part of that certification, it must maintain control of its documentation. These documents include system (or applications) user manuals, hardware manuals, quality (which include security) policies, standards, procedures, and approvals. It must maintain a list of master documents, which serves as approved references for work processes, and a list of quality records, which document the quality of the output products.

The FSA SSO controls the SAIG Continuity of Support/Disaster Recovery Plan, the SAIG System Security Plan, and SAIG Risk Assessments.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

Mailboxing
48) List documentation and its location for SAIG, including:

- *Documentation for vendor-supplied hardware/software,*
- *Application security plans,*
- *Test procedures and results,*
- *SOPs,*
- *Emergency procedures.*

3.8 Security Awareness Training

FSA does not conduct SAIG specific security training at this time.

VDC employees are mandated to attend annual security briefing sessions. The Security Awareness Briefing lasts approximately 1 hour. Additionally, all new hires attend a briefing on security access. The Security Access Briefing focuses on CSC badge and physical access requirements.

Security Awareness Briefing are held annually and may include the following topics as part of the Security Briefing:

- Description of CSC Security Program
- Proprietary Data Security Program
- Access Control
- Property Removal
- National Industrial Security Program
- International Traffic and Arms Regulation
- Social Engineering

Other relevant topics are delivered on an as needed basis. Attendance at these briefings is mandatory for VDC personnel.

FSA employees are required to attend annual information security awareness training that is adequate to fulfill their security responsibilities. The SAIG SSO receives monthly training on procedures relating to security and privacy by the FSA Security and Privacy team.

FSA assures that their employees and contractor personnel have been provided adequate training by bringing in contracted subject matter experts to conduct the training sessions and by complying with federal and departmental policies and procedures for the training.

As of November 8, 2002, the below issue remains outstanding. Once the information is provided, the SSO should insert the answers into this section

> Does Mod Partner have security awareness training? If so, how often is it given and to whom?

3.9 Incident Response Capability

Identification
The VDC uses ISS Real Secure©, Tripwire for Servers©, IBM Resource Access Control Facility (RACF©), Technologic, Inc. Smart Security Administrator©, CA Top Secret©, BMC Enterprise Security Station© Norton Anti-Virus©, and CA UniCenter TNG©, as

intrusion detectors and system scanners. System and Network Administrators review the audit logs on daily basis for unusual activities or immediately in the case of an actual attack.

Reporting

Physical security incidents are reported to the on-site VDC Security Officer for validation as per *NDC/MDC Security Investigation Procedure.* These incidents are typically theft or destruction of data, computer equipment, storage devices, or proprietary information. Others incidents might be fire, flood, hurricane, or terrorist attack.

All computer and network related security incidents (e.g. virus, back door, Trojan horses, intrusion, hacks, denial of service, etc) are reported to the CSC Computer Emergency Response Co-ordination Center (CERCC) and up the CSC management chain as per *GISS Policy 19 SP-I013 Virus Protection Plan* as well as Federal Computer Incident Response Center (FedCIRC) and FSA VDC Security Officer. FSA VDC Security Officer will notify the following agencies, as appropriate:

- Federal Bureau of Investigations (FBI)/National Infrastructure Protection Center (NIPC)
- IG Criminal Division
- GSA Federal Protective Service (FPS)

The CSC Computer Emergency Response Co-ordination Center (CERCC) was formed to coordinate and track responses to all computer security events such as break-ins, virus outbreaks and inappropriate or unauthorized use of computing resources. The Center maintains the most current anti-virus software updates (e.g. patches) and virus definitions at security.csc.com. The CSC CERCC maintains the "*CERCC Alerts & Bulletins*" database, which contains Virus, Hoaxes, Trojans, and other Security Alerts and Bulletins. The Data and Network Security Administrators check the CSC CERCC on a regular basis for news on virus and the latest security patches.

All attempts are made to preserve all the artifacts of an attack for law enforcement agencies. The attacked server is disconnected and its back-up server placed online to maintain system(s) availability. User IDs involved in the attack will be disabled but not deleted.

Patch Maintenance

Upon receiving a security alert notification, the VDC updates a Security Status spreadsheet. The technical lead performs a security impact assessment to determine exposure risk. If risk of exposure to the threat and/or vulnerability is minimal, then the security status spreadsheet is updated to reflect that fact. If not, the change control review board (CCRB), with client and vendor concurrence, will initiate a change in system configuration to address the risk.

See section 3.9 of the VDC SSP dated June 2002 for additional information about Incident Response and the procedures to follow in responding to an incident.

For enrollment see section 3.9 of the CPS SSP dated July 2002 for information about Incident Response and the procedures to follow in responding to an incident.

4.0 Technical Controls

Technical controls focus on security controls that the computer system executes. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

4.1 Identification And Authentication

At this time there are no other ways to correlate SAIG actions to users besides TG numbers (user ID's) and passwords.

Inactive user ID's for SAIG are not automatically disabled; however, passwords must be changed after 120 days.

SAIG's only authentication control mechanism is the use of assigned user ID's and passwords. The system does not use biometrics, token controls or digital or electronic signatures.

Current password policy for SAIG passwords is:

- Password must be 7 or 8 characters in length
- Valid characters must be from the 7-bit US-ASCII character set,
- Begin with an alpha character,
- Contain only alphanumeric characters,
- Password expires 120 days after being changed
- Password change forced when using default password

Password changes are forced when using the original default password on first use and they expire 120 days after being changed. There is no set limit as to when passwords may be changed again.

There is no limit to the number of invalid access attempts that may occur for a given user ID; therefore, there is no lockout mechanism for SAIG.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

> *61) Describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator). ?*
>
> *62) Describe the level of enforcement of the access control mechanism (network, operating system, and application).*

63) Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual). Please clarify the role of the Destination Point Administrators and how they administer the passwords of the schools, GA's etc.

64) Describe the self-protection techniques for the user authentication mechanism (e.g., passwords re transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).

65) Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

66) What are the procedures for limiting scripts with embedded passwords?

67) Are there policies that provide for the bypassing of user authentication requirements, single-sign-on technologies and any compensating controls?

4.2 Logical Access Controls

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

68) Discuss controls in place to authorize or restrict the activities of users and system personnel within SAIG.

69) Describe software features that are designed to permit only authorized access to or within the system to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

70) Describe formal policies that define the authority that will be granted to each user or class of users. Do these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more?

71) Do the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion?

72) Describe the system's capability to establish an Access Control List or register of the users and the types of access they are permitted.

73) Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

74) Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

75) Indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application?

76) Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users?

77) Describe the controls used to detect unauthorized transaction attempts by authorized and/or unauthorized users.

78) Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before continuing.

79) Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends?

80) Is encryption used to prevent unauthorized access to sensitive files as part of the system or application access control procedures?

81) Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.

82) Indicate if host-based authentication is used.

83) Is a standardized log-on banner used by the system?

84) Are warning messages displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment?

85) What is the rationale for electing to use or not use warning banners and provide an example of the banners used?

4.3 Audit Controls

UNIX, NT, and network servers have continuous event logging capability though their operating systems. The auditing subsystem protects itself against unauthorized access by using appropriate authentication mechanisms. Audit logs do not record personal information about users and no keystroke monitoring tools are used. Additional auditing capabilities of the VDC are detailed below.

Network
The ISS Real Secure© intrusion detection engine monitors and scans the network. All events are written to a log audit file that resides on a secure hard drive. System Administrators review the logs twice daily and on an as needed basis.

NT
The NT operating system keeps a security audit log of users activities. The audit policy, controlling the types of events that are recorded in the security log, is set by the system administrator. The events that are monitored are logon attempts, logoffs, file access, object (or resource) access, use of user rights, user and group management, security policy changes, restart, shutdown, and process tracking. The System Administrator reviews audit logs on a daily basis. These audit logs also help to identify other problems such as hardware failures and application problems. Access to the logs is restricted to the Administrators group only. The system administrator reviews the audit trails following a known system or application software problem, a known violation of requirements by a user, or some unexplained user problem. SAIG audit trails, per FSA policy, are capable of being queried by user ID, terminal ID, application name, date and time, or some other set of parameters. The native event viewer in Windows NT has the ability to filter out events that do not meet the requested criteria. The choices by which to filter are date/time, user ID, Computer name, and Event ID. The ability to search for specific application events is limited by the “Source” drop down menu of the event viewer filter screen. Additionally, VDC NT systems use Tripwire for Servers© as an Intrusion Detector to monitor changes due to intruders. Norton Antivirus© software checks the system for viruses.

HP-UNIX

All SAIG system activities on the HPUX server are logged via the syslog daemon. User logins (logged along with source IP address in /var/adm/syslog/syslog.log) and actions are logged by standard HP utilities and can be traced in order to support accountability and support after-the-fact investigations of how, when, and why normal operations ceased. These audit logs can also be used for a variety of troubleshooting scenarios. Audit logs are strictly controlled since only “root” has the ability to read the logs. Audit logs are reviewed on an as-needed basis especially. The system administrator reviews the audit trails following a known system or application software problem, a known violation of requirements by a user, or some unexplained user problem. A VDC security team processes requests as they relate to access control functions and a system administrative

team implements the requests. Additionally, VDC UNIX systems use Tripwire for Servers© as an Intrusion Detector to monitor changes made by intruders.

SAIG Portal

The Oracle database contains many tables used for auditing data transmissions, database access, and the different levels of access with the TDCommunityManager administration tool. Appropriate Oracle tables maintain an audit trail of all activity. This includes who files are sent to, who files are received from, file sizes, file transfer duration, etc. Listed below are some of the table names and descriptions that the auditing process incorporates:

Mailbox_Logon – This table contains the SECOFR, System Administrator and Accounts detail.

- *SECOFR* – Refers to the level of TDCM user, accessed only via a local installation of TD Manager, not TDCM. Used by System Administrators.
- *System Administrator* - Refers to the level of TDCM user with the ability to verify all Accounts and Participants in the Oracle database.
- *Accounts* - Refers to the level of TDCM user with the ability to verify all Participant mailbox contents, but not able to see other Accounts in the Oracle database.

Mailbox_Log – This table contains Administration traffic, invalid and valid logon attempts in the TDCM administration tool, and affected or changed user ID details in the Oracle database.

Mailbox_Log_Status – This table contains all sent and received activity and tracks each transaction giving a detailed account of each data transmission on the Portal in regards to transmitted data. This transmission data is indexed via a unique 20-digit filename that is used as a key to the entire SAIG Portal.

Mailbox_Transtbl – This table stores via the unique 20 digit filename used during the send/receive, query_list (i.e. gives a "listing of the mailbox and status of data") and provides a more detailed account of all transactions occurring for a given account. It is not limited to the transmission of files similar to those in the Mailbox_Log_Status table.

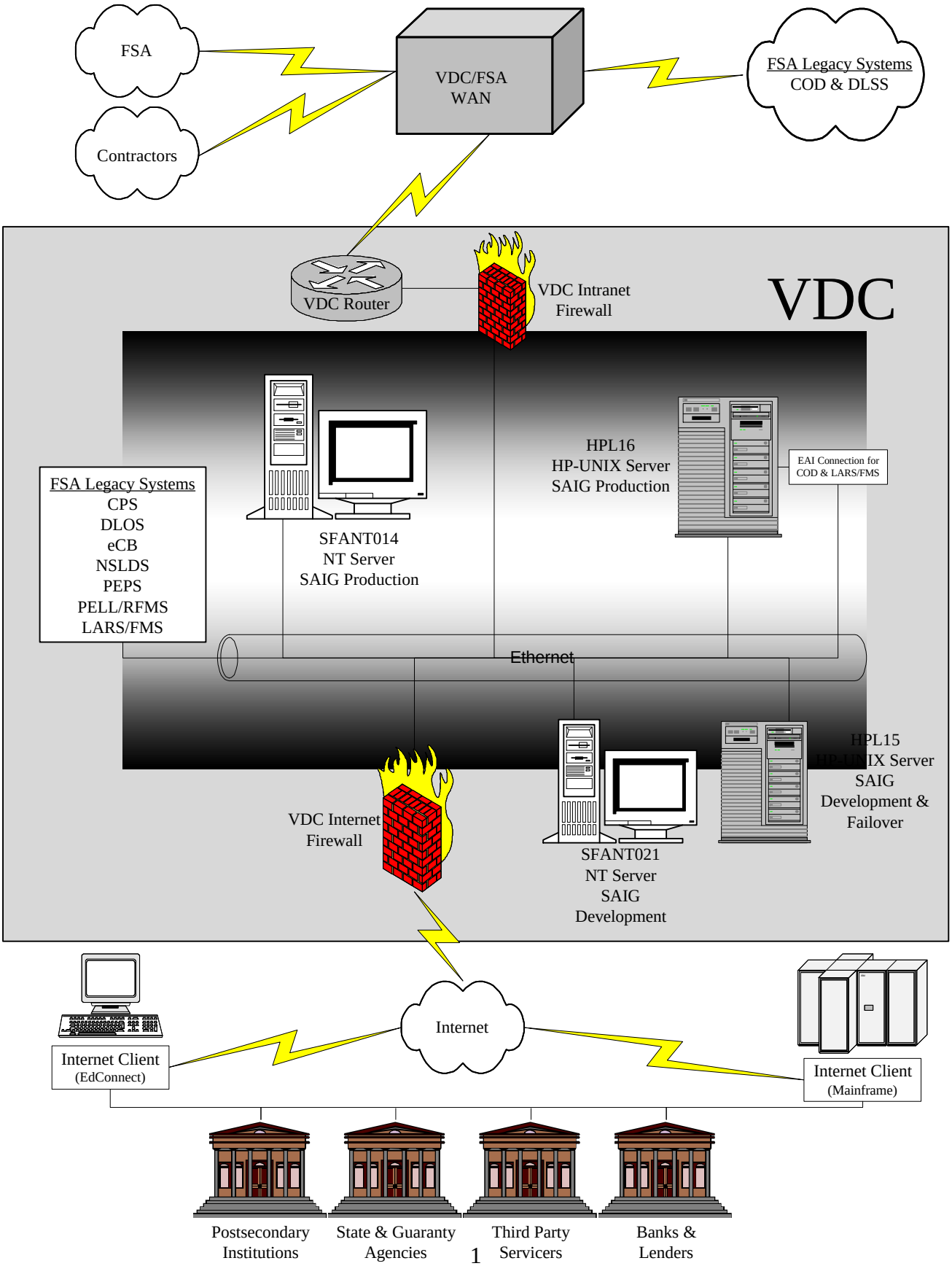
SAIG Enrollment

The stderr.log, event.log, and stdout.log that JRun writes to file on the Web host machine at the VDC is the primary means of audit trail creation and logging used by the SAIG Web Enrollment site. All debug and JRun system statements are recorded in these files. These files are archived and cleaned out on a weekly basis by VDC administration. These files and all firewall, FTP, and telnet security in place by VDC are protected by Windows NT security.

As of November 8, 2002, the below questions remain outstanding. Once the information is provided, the SSO should insert the answers into this section

86) Do FSA or NCS personnel have any role in reviewing the audit logs or is the process controlled entirely by the VDC?

Appendix A: SAIG Logical Network Diagram



Appendix B: Additional HP-UNIX Midtier Software

Object COBOL/UX Developer Bundle for HPUX 11.0
MirrorDisk/UX
HP GlancePlus/UX Pak for s800 11.00
HP Process Resource Manager
HP C/ANSI C Developer's Bundle for HP-UX 11.00 (S800)
HP aC++ Compiler (S800)
Special Edition HP-UX Unlimited-User Lic
HP OnLineJFS (Advanced VxFS)
MC / Service Guard
HP PerfView Analyzer for s800 11.00
HP-UX Development Kit for Java*
HP-UX Installation Utilities (Ignite-UX)
HP Cluster Object Manager
HP-UX ServiceControl Manager - Integrated Agent Software
Java 2 SDK 1.3 for HP-UX (700/800), PA1.1 + PA2.0 Add On
Java 2 RTE 1.3 for HP-UX (700/800), PA1.1 + PA2.0 Add On
English HP-UX 64-bit Runtime Environment
HP-UX Installation Utilities for Installing 11.00 Systems
Netscape Fasttrack Server
PCI RS-232 MUX Software
Netscape Enterprise Server
Netscape US/Canada
HPUX 11.0 Support Tools Bundle, Jun 2001
HP-UX General Release Patches, March 2001
HP-UX Hardware Enablement and Critical Patches, September 2001
Perl Programming Language
Node Agent Configuration for SCMgr
MQSeries for HP-UX
MQSeries Update (U474386) for HP-UX
MQSeries Update (U474837) for HP-UX
HP OpenView OmniBack II